E-5272-01EK

A METHOD FOR MANAGING PUBLIC KEY

BACKGROUND OF THE INVENTION

本発明は、公開鍵の管理方法に係り、特に、ネットワークにおけるセキュリティ技術に使用される公開鍵暗号システムに使用して好適な公開鍵の管理方法に関する。

インターネットを使用してセキュリティ通信を実現する方法として、例えば、ＩＰ(Internet Protocol)レイヤのセキュリティプロトコルであるＩＰＳＥＣ(IP SECurity) がある。ＩＰＳＥＣに関する技術文献として、例えば、IETF(Internet Engineering Task Force) 発行の [RFC1825] "Security Architecture for the Internet Protocol." (R.Atkinson著)等が知られている。

ＩＰＳＥＣに付随する鍵管理プロトコルは、公開鍵暗号システムを利用するものである。鍵管理プロトコルに関する従来技術として、例えばIETF発行の "Simple Key-Management For Internet Protocol." (著者：Ashar Aziz, Tom Markson, Hemma Prafullchandra)等に記載されたＳＫＩＰと呼ばれる技術が知られている。以下、この鍵管理プロトコルについて説明する。

いま、ネットワーク内にセキュリティ通信を行う２つのホストＡ、Ｂがあり、これらのホストＡ、Ｂは、ＩＰＳＥＣに基づいた共通鍵暗号システムによって暗号通信を行うものとし、ホストＡは、ホストＢの公開鍵を、ホストＢは、ホストＡの公開鍵を知っているものとする。

ホストＡとＢとは、通信を行うに際して、既知のアルゴリズムを用いてそれぞれ自らの秘密鍵と相手の公開鍵とを組み合わせて共通鍵を暗号化するための鍵Ｋ(Ａ)、Ｋ(Ｂ)を生成する。ここで、例えば、ホストＡがホストＢにデータを送信するとき、ホストＡは、共通鍵Ｔを生成し、それを用いてデータを暗号化し、鍵Ｋ(Ａ)を用いて共通鍵Ｔを暗号化する。ホストＡは、暗号化された共通鍵Ｔの情報を含む新たなヘッ

ダをＩＰヘッダの後に挿入する。受信側のホストＢは、自らが持つ秘密鍵によって、パケットの中にある暗号化された共通鍵Ｔを解読し、解読した共通鍵Ｔによって暗号化されたパケットのデータを解読する。そして、このようなホストＡ、Ｂ間のセキュリティ通信において、データを暗号化するための共通鍵は、定期的に更新される。

前述したようなＩＰＳＥＣに付随する従来技術による鍵管理プロトコルは、セキュリティ通信を行う２つのホストが通信開始前に互いに相手の公開鍵を知っていることが前提とされている。

前述した従来技術による方法は、セキュリティ通信を行おうとする２つのホストが、通信開始前にお互いの公開鍵を自動的かつ安全に交換する方法がなく、その結果、手渡しによる公開鍵の交換等の方法に頼ることになり、公開鍵の管理が複雑になっているという問題点を有している。また、この結果、前述の従来技術は、ネットワークの規模が大きい場合、ネットワークの管理者に対する負担が大きくなるという問題点を生じさせている。

さらに、前述の従来技術は、ネットワーク上の認証を伴わない公開鍵の配布を行った場合、不正なホストがセキュリティ通信の相手になりすますことを防ぐことができないという問題点をも有している。

SUMMARY OF THE INVENTION

本発明の目的は、前述した従来技術の問題点を解決し、セキュリティ通信を行おうとする２つのホストが通信開始前にお互いの公開鍵を自動的かつ安全に交換することを可能にした公開鍵の管理技術を提供することにある。

本発明によれば前記目的は、階層構造を持ち、各階層毎にドメイン名を持つネットワークと、そのドメイン名とアドレスとの対応を管理する前記各階層毎に設けられるＤＮＳサーバと、ネットワークに収容されるホストとを備え、前記ＤＮＳサーバが、ネットワークに属するホストに対して他のホストが持つ公開鍵を配布する公開鍵管理システムにおいて、前記ＤＮＳサーバが、公開鍵を管理する手段と、前記ネットワ

ークに属するホストの公開鍵とドメイン名とを対応付けて格納するデータベースとを備え、第１のホストからのドメイン名の情報による第２のホストの公開鍵の問い合わせを受けたとき、前記公開鍵管理手段が前記データベースを参照することにより、前記ドメイン名に対応する第２のホストの公開鍵の情報を前記第１のホストに応答することにより達成される。

また、前記目的は、前記ＤＮＳサーバが、第１のホストから第２のホストの公開鍵の問い合わせを受けたとき、自サーバ内の前記データベースの中に問い合わせのドメイン名に対応するエントリがない場合、他の公開鍵管理手段とデータベースとを備えた他のＤＮＳサーバに公開鍵の解決をドメイン名の階層に沿って再帰的に委託することにより達成される。

さらに、前記目的は、前記ホストが、前記ＤＮＳサーバに他のホストの公開鍵を問い合わせる手段を備え、セキュリティ通信開始時、前記公開鍵問い合わせ手段に通信相手となるホストのドメイン名に対応する公開鍵を前記ＤＮＳサーバに問い合わせることにより達成される。

本発明の目的は、前述の手段を持つ構成以外に、さらに、次に示すような手段を備えることによっても達成することができる。

すなわち、前記目的は、ネットワークの構成に変更が生じた場合、構成の変化に関係する一部のＤＮＳサーバが、ホストの公開鍵とドメイン名のと対応を格納しているデータベースを更新し、前記以外のＤＮＳサーバがデータベースの更新を行わないようにすることにより達成される。

また、前記目的は、前記公開鍵管理手段とデータベースとを備えたＤＮＳサーバと、前記公開鍵を問い合わせる手段を備えたホストとに電子署名を処理する手段を設け、公開鍵問い合わせ及び応答のために出力するパケットに電子署名を付け、電子署名の付いた入力パケットについて、その電子署名を確認し、改竄されている入力パケットを廃棄することにより、パケットの内容が改竄されるのを防止するようにすることにより達成される。

また、前記目的は、公開鍵問い合わせ及び応答のために上記公開鍵管理手段とデータベースとを備えたＤＮＳサーバと、前記公開鍵を問い合わせる手段を備えたホストとが、入出力するパケットとして、従来のＤＮＳパケットと同じフォーマットのパケットを用いることにより達成される。

また、前記目的は、前記ＤＮＳサーバに対してホストが送信する公開鍵問い合わせパケットの中にホストが信用するＤＮＳサーバのドメイン名の情報を含め、公開鍵の情報を応答する前に、前記ＤＮＳサーバの公開鍵管理手段に、公開鍵問い合わせパケットの中で示されるホストが信用するＤＮＳサーバに対して電子署名を要求させ、電子署名の要求を受けたＤＮＳサーバの公開鍵管理手段に、公開鍵応答パケットに電子署名を付けさせ、その電子署名により公開鍵応答パケットに含まれる公開鍵の情報が信用できるか否かを前記ホストの電子署名を処理する手段に判定させ、これにより、不正なホストが自分の公開鍵とアドレスとを公開鍵問い合わせパケットの中にある問い合わせドメイン名に対応しているように見せかけることを防止するようにしたことにより達成される。

また、前記目的は、電子署名の要求を受けたＤＮＳサーバが公開鍵問い合わせパケットの中で示されるホストが信用するＤＮＳサーバと異なるとき該ＤＮＳサーバの公開鍵管理手段は、ドメイン名の階層構造に沿って、上位のＤＮＳサーバに公開鍵応答パケットに対する電子署名を要求し、最終的には公開鍵問い合わせパケットの中で示されるホストが信用するＤＮＳサーバに公開鍵応答パケットに電子署名を付けさせることにより達成される。

また、前記目的は、前記ホストの公開鍵問い合わせ手段に、問い合わせるドメイン名に従って信用するＤＮＳサーバを選択させ、公開鍵問い合わせパケットの中に該ＤＮＳサーバのドメイン名の情報を含め、公開鍵応答パケットに電子署名を付ける処理を行うＤＮＳサーバの数を減らすことにより公開鍵の取得を効率的なものとすることにより達成される。

また、前記目的は、電子署名付きの公開鍵の応答を受けたＤＮＳサーバの公開鍵

管理手段に、電子署名付きの公開鍵の応答パケットに含まれる公開鍵、電子署名及び電子署名をしたサーバのドメイン名の情報をキャッシングさせ、ネットワーク及びサーバに無駄な負荷がかかることを防止し、公開鍵の取得を効率化するようにしたことにより達成される。

前述において、ネットワークのドメイン名とアドレスとの対応を解決する手段であるＤＮＳは、ＤＮＳを実現するための装置であるＤＮＳサーバの機能を拡張し、ドメイン名と公開鍵との対応を解決する手段を提供する。ＤＮＳの実現方法は、例えば、IETF 発行の文献［RFC1035］“ Domain Names - Implementation and Specifications”(著者：P. Mockapetris)等に説明されている。

本発明により公開鍵を管理する手段と、ネットワークに属するホストの公開鍵とドメイン名とを対応付けて格納されたデータベースとを有する機能拡張されたＤＮＳサーバは、ホストからドメイン名の情報によって公開鍵の問い合わせを受けたとき、前記の公開鍵を管理する手段が前記データベースを参照することにより、問い合わせのドメイン名に対応する公開鍵をホストに応答することができる。これにより、本発明は、ネットワーク上の２つのホストがセキュリティ通信を開始するとき、通信相手のホストのドメイン名に対応する公開鍵を自動的に取得させ、ネットワークにおける公開鍵の管理を容易とすることができる。

また、本発明は、公開鍵問い合わせパケットの中にホストが信用するＤＮＳサーバの名前を入れさせ、このホストが信用するＤＮＳサーバによって公開鍵応答パケットに電子署名を付けさせているので、公開鍵応答パケットにある公開鍵が信用できるか否かをホストが判定することができ、不正なホストが自分の公開鍵とアドレスが問い合わせのあったドメイン名に対応しているように見せかけることでセキュリティ通信の相手になりすますことを防止することができる。このとき、公開鍵を取得するためにやり取りする全てのパケットに対して、前述した機能拡張したＤＮＳサーバに電子署名を付けさせることにより、パケットの内容の改竄を防止することができる。

BRIEF DESCRITPTION OF THE DRAWINGS

図１は本発明の一実施形態におけるＫＭＳ(Key Management Server)の構成を示すブロック図である。

図２は上記実施形態におけるＤＮＳクライアントの機能を持つホストの構成を示すブロック図である。

図３は上記実施形態における公開鍵とドメイン名との対応を説明するテーブルの構成を示す図である。

図４はＤＮＳサーバが公開鍵の問い合わせを受けたときに公開鍵を応答する手順を説明するフローチャートである。

図５はＤＮＳサーバが電子署名の要求を受けたときに公開鍵応答パケットに電子署名を付与する手順を説明するフローチャートである。

図６はＤＮＳクライアントの機能を持つホストが通信相手の公開鍵を取得する手順を説明するフローチャートである。

図７は本発明を階層的なドメイン名の構造を持つネットワークに適用した場合の実施形態を示すブロック図である。

図８はホストが通信相手の公開鍵の取得ために行う手順の中で、ホスト・ＫＭＳ間及びＫＭＳ・ＫＭＳ間でやり取りするパケットの種類とそれらに付与される電子署名を説明する図である。

図９はＤＮＳパケットのフォーマットの構成を説明する図である。

図１０はＤＮＳパケットに含まれる資源レコードのフォーマットの構成を説明する図である。

DESCRIPTION OF THE EMODIMENTS

以下、本発明を用いた公開鍵管理システムの実施形態を図面を参照して詳細に説明する。

図１は本発明の一実施形態の公開鍵管理システムにおけるＫＭＳ(Key Management Server)の構成を示すブロック図、図２はＤＮＳクライアントの機能を持つホストの構成を示すブロック図である。ＫＭＳはＤＮＳサーバを機能拡張したサーバである。同様に、上記ホストは機能拡張したＤＮＳクライアントの機能を持つ。図３は公開鍵とドメイン名との対応を説明するテーブルの構成を示す図、図４はＤＮＳサーバが公開鍵の問い合わせを受けたときに公開鍵を応答する手順を説明するフローチャート、図５はＤＮＳサーバが電子署名の要求を受けたときに公開鍵応答パケットに電子署名を付与する手順を説明するフローチャート、図６はＤＮＳクライアントの機能を持つホストが通信相手の公開鍵を取得する手順を説明するフローチャート、図７は本発明を階層的なドメイン名の構造を持つネットワークに適用した場合の実施形態を示すブロック図、図８はホストが通信相手の公開鍵の取得ために行う手順の中で、ホスト・ＫＭＳ間及びＫＭＳ・ＫＭＳ間でやり取りするパケットの種類とそれらに付与される電子署名を説明する図、図９はＤＮＳパケットのフォーマットの構成を説明する図、図１０はＤＮＳパケットに含まれる資源レコードのフォーマットの構成を説明する図である。図１、図２、図７、図８において、１０はＫＭＳ、１１、２１はネットワーク制御部、１２、２２はＩＰ処理部、１３、２３はＴＣＰ／ＵＤＰ処理部、１４は拡張ＤＮＳ処理部、１５はドメイン名／ＩＰアドレステーブル、１６、２５はドメイン名・公開鍵・電子署名テーブル、１７、２６は初期保持データ、２４は拡張ＤＮＳクライアント、２７はセキュリティ通信処理部、１０１はネットワーク、１４１、２４１はＤＮＳパケット振り分け部、１４２はＤＮＳ処理部、１４３は公開鍵問い合わせ／応答処理部、１４４は電子署名処理部、２４２はドメイン名リゾルバ、２４３は公開鍵問い合わせ処理部、２４４は電子署名処理部、７１、７５はホストＡ、Ｂ、７２～７４、７６はＫＭＳである。

まず最初に、本発明が適用されるネットワークシステム全体の構成及び処理の流れについて図７を参照して説明する。

図７に示すネットワークシステムは、ネットワークが階層構造を持ち、各階層毎

にドメイン名が与えられており、ドメインを持つネットワークの各階層が１つのＫＭＳを持つように構成されている。ここで、ホストＡ７１がホストＢ７５の公開鍵を取得する場合について考える。この場合、ホストＡ７１は、同一のドメインの階層にあるＫＭＳ１(７２)に対してホストＢ７５の公開鍵を問い合わせる。このとき、単にホストＢ７５の公開鍵のデータを受け取るのみでは不正な他のホストがホストＢ７５に成りすますのを防ぐことができないので、ホストＡ７１は、信用することができるＫＭＳの電子署名も要求する。今の場合、ホストＡ７１が信用するＫＭＳはＫＭＳ００(７４)であるとする。また、ＫＭＳ００(７４)の公開鍵は、ホストＡ７１のみならず一般に広く知られ、認証されているものとする。

ホストＡ７１がホストＢ７５の公開鍵のデータを要求すると、ＫＭＳ１(７２)はこの要求に対して、ホストＢ７５の公開鍵のデータを持っている場合、ホストＡ７１が信用しているＫＭＳ００(７４)にホストＢ７５の公開鍵のデータに電子署名を付けるように要求する。一方、ＫＭＳ１(７２)は、ホストＢ７５の公開鍵のデータを持ってない場合、上位のＫＭＳ０(７３)に問い合わせる。その際、ホストＢ７５の公開鍵のデータを持っているＫＭＳに行き会うまで再帰的に上位のＫＭＳへの問い合わせが続けられる。ＫＭＳ１(７２)からの問い合わせを受けたホストＢ７５の公開鍵のデータを持っているＫＭＳは、ＫＭＳ００(７４)に電子署名を要求する。

電子署名を付けるように要求されたＫＭＳ００(７４)は、自らの電子署名を付けたホストＢ７５の公開鍵のデータをＫＭＳ１(７２)に返す。ＫＭＳ１(７２)は、ホストＢ７５の公開鍵のデータをホストＡ７１に返す。この場合、ホストＡ７１は、元々ＫＭＳ００(７４)の公開鍵を知っているためそれが信用できるデータか否かを判断することができる。

前述した一連の処理によりホストＡ７１は、ホストＢ７５の公開鍵を安全に取得することができ、これを使用して、ホストＢ７５との間でセキュリティ通信を行うことができる。

次に、図９、図１０を参照して、ＤＮＳパケットのフォーマットの構成と、ＤＮ

Ｓパケットに含まれる資源レコードのフォーマットの構成とを説明する。

ＤＮＳパケットは、図９に示すように、ＤＮＳヘッダ９１、問い合わせ部９２、回答部９３、権限付きネームサーバの名前を表す権威部９４、複数の資源レコードを含む付加情報部９５から成る。また、図１０に示すように、ＤＮＳパケットに含まれる資源レコードの１つであるＴＸＴレコードは、名前フィールド１０１、ＴＹＰＥフィールド１０２、ＣＬＡＳＳフィールド１０３、この資源レコードが捨てられずにキャッシュされている時間間隔を示すＴＴＬフィールド１０４、データ長フィールド１０５、データフィールド１０６からなる。

複数の資源レコードとしては、ＴＹＰＥにより識別される複数のものがあり、本発明の実施形態においては、複数あるＤＮＳ資源レコードの内ＴＸＴレコードと呼ばれるＴＹＰＥ＝１６の資源レコードに、公開鍵問い合わせ情報及び公開鍵応答情報を入れることとする。また、本発明の実施形態は、公開鍵問い合わせ情報及び公開鍵応答情報を入れる資源レコードのデータフィールド１０６の先頭に公開鍵問い合わせ／応答、電子署名要求、または、通常のＴＸＴレコードの区別がつくような識別子１０６１のフィールドを設けている。

なお、ＴＸＴレコードについては、前掲のＤＮＳに関する文献の中に説明がある。また、資源レコードとして、前述したＴＸＴレコードの他に、アドレスとドメイン名との対応を示すＡレコード（ＴＹＰＥ＝１）、メール・エクスチェンジャのドメイン名を示すＭＸレコード（ＴＹＰＥ＝１５）等がある。

次に、図１を参照して、本発明の実施形態によるサーバであるＫＭＳの構成を説明する。図１において、各ブロックを結ぶ実線はパケットの受け渡しを行う関係を示し、破線はデータの参照を行うことを示す。

ＫＭＳ１０は、ネットワーク制御部１１と、ＩＰ処理部１２と、ＴＣＰ／ＵＤＰ処理部１３と、拡張ＤＮＳ処理部１４と、ドメイン名・ＩＰアドレステーブル１５と、ドメイン名・公開鍵・電子署名テーブル１６と、初期保持データ１７とを備えて構成され、ネットワーク制御部１１を介してネットワーク１０１に接続されている。また、

拡張ＤＮＳ処理部１４は、ＤＮＳパケット振り分け部１４１と、ＤＮＳ処理部１４２と、公開鍵問い合わせ／応答処理部１４３と、電子署名処理部１４４とを備えて構成されている。

前述において、ネットワーク制御部１１は、ＫＭＳ１０とＩＰネットワーク１０１とを接続している。ＩＰ処理部１２は、ネットワーク制御部１１の上位にあって、ＩＰ(Internet Protocol) によってやり取りされるパケットの送受信処理を行う。ＴＣＰ／ＵＤＰ処理部１３は、ＩＰ処理部１２の上位にあって、ＴＣＰ／ＵＤＰ(Transmission Control Protocol／User Datagram Protocol) によってやり取りされるパケットの送受信処理を行う。ここで、特に、ＴＣＰ／ＵＤＰ処理部１３は、ＤＮＳに割り当てられたソケット番号を持つパケットを受信したとき、そのパケットを拡張ＤＮＳ処理部１４に送る。逆に、拡張ＤＮＳ処理部１４は、自ら生成したパケットを送信するとき、その送信すべきパケットをＴＣＰ／ＵＤＰ処理部１３に送る。

拡張ＤＮＳ処理部１４におけるＤＮＳパケット振り分け部１４１は、ＴＣＰ／ＵＤＰ処理部１３からＤＮＳパケットを受け取り、図１０に示す識別子１０６１を見てＤＮＳ処理部１４２、公開鍵問い合わせ／応答処理部１４３、電子署名処理部１４４の内のどれかにＤＮＳパケットを振り分ける。ＤＮＳ処理部１４２は、ＴＣＰ／ＵＤＰ処理部１３からの従来のＤＮＳパケットを受け取り、ドメイン名とＩＰアドレスとが対応づけて格納されているデータベースであるドメイン名・ＩＰアドレステーブル１５の検索またはエントリの追加を行う。公開鍵問い合わせ／応答処理部１４３は、他のＫＭＳからの公開鍵の問い合わせを拡張ＤＮＳパケットの形でＴＣＰ／ＵＤＰ処理部１３から受け取ったとき、問い合わせのあったドメイン名の公開鍵を取得するためにドメイン名と公開鍵とが対応づけて格納されたドメイン名・公開鍵・電子署名テーブル１６を検索する。

ドメイン名・公開鍵・電子署名テーブル１６は、図３に示すように、ドメイン名３１、公開鍵３２、ホストが信用するＫＭＳが付けた電子署名３３、電子署名を付けたＫＭＳのＫＭＳ名３４、エントリの生成時点を示すタイムスタンプ３５の５つの項

目を含む。公開鍵問い合わせ／応答処理部１４３は、もし、ドメイン名・公開鍵・電子署名テーブル１６にエントリがあれば、問い合わせの要求に従って他のＫＭＳへ電子署名の要求を出すか、または、電子署名処理部１４４によって公開鍵の応答パケットに電子署名を付ける処理を行う。また、公開鍵問い合わせ／応答処理部１４３は、ドメイン名・公開鍵・電子署名テーブル１６にエントリがないとき、ＴＣＰ／ＵＤＰ処理部１３を介して他のＫＭＳに対して、問い合わせのあったドメイン名の公開鍵を問い合わせるパケットを送信する。電子署名処理部１４４は、他のＫＭＳからの電子署名要求を拡張ＤＮＳパケットの形でＴＣＰ／ＵＤＰ処理部１３から受け取ったとき、問い合わせの要求に従って他のＫＭＳへ電子署名の要求を出すか、または、公開鍵応答パケットに電子署名を付ける処理を行う。

また、ＫＭＳ１０は、初期保持データ１７を保持している。初期保持データ１７は、自分のドメイン名・公開鍵１７１、ＤＮＳの親子関係において上位のＫＭＳのドメイン名１７２、ＤＮＳの親子関係において下位にあるものの中で信用するＫＭＳのドメイン名・公開鍵１７３から成る。ＫＭＳ１０は、他のＫＭＳに公開鍵を問い合わせに行くときにこれらのデータを利用する。

次に、図２を参照して本発明により拡張したＤＮＳクライアントの機能を持つホストの構成を説明する。

ホスト２０は、ネットワーク制御部２１と、ＩＰ処理部２２と、ＴＣＰ／ＵＤＰ処理部２３と、拡張ＤＮＳクライアント２４と、ドメイン名・公開鍵・電子署名テーブル２５と、初期保持データ２６と、セキュリティ通信処理部２７とを備えて構成され、ネットワーク制御部１１を介してＩＰネットワーク１０１に接続されている。また、拡張ＤＮＳクライアント２４は、ＤＮＳパケット振り分け部２４１と、ドメイン名リゾルバ２４２と、公開鍵問い合わせ処理部２４３と、電子署名確認部２４４とを備えて構成されている。

前述において、ホスト２０は、ＫＭＳと同様に、ネットワーク制御部２１、ＩＰ処理部２２、ＴＣＰ／ＵＤＰ処理部２３を持ち、ＩＰネットワーク２０１に接続され

ている。ＴＣＰ／ＵＤＰ処理部２３は、ＤＮＳに割り当てられたソケット番号を持つパケットを受信したとき、そのパケットを拡張ＤＮＳクライアント２４に送る。逆に、拡張ＤＮＳクライアント２４は、自ら生成したパケットを送信するとき、そのパケットをＴＣＰ／ＵＤＰ処理部２３に送る。

拡張ＤＮＳクライアント２４内のＤＮＳパケット振り分け部２４１は、ＴＣＰ／ＵＤＰ処理部２３からＤＮＳパケットを受け取り、ＤＮＳヘッダの中身を見てドメイン名リゾルバ２４２、公開鍵問い合わせ処理部２４３のいずれかに処理を振り分ける。ドメイン名リゾルバ２４２は、従来のＤＮＳクライアントと同様に、ドメイン名に対応するＩＰアドレスを解決する処理を行う。そして、ドメイン名に対応するＩＰアドレスを問い合わせる際、ドメイン名リゾルバ２４２は、ＴＣＰ／ＵＤＰ処理部２３を通して問い合わせパケットを送信する。ドメイン名リゾルバ２４２は、問い合わせに対する応答もＴＣＰ／ＵＤＰ処理部２３を通して受信する。

本発明により新たに付加したモジュールである公開鍵問い合わせ処理部２４３は、ドメイン名に対応する公開鍵を解決する処理を行う。公開鍵問い合わせ処理部２４３は、新規に得た公開鍵の情報をドメイン名・公開鍵・電子署名テーブル２５に保存し、次回に公開鍵を問い合わせに行く前に参照する。電子署名確認部２４４は、公開鍵問い合わせ処理部２４３が受け取った公開鍵の情報について、初期保持データ２６内の信用するＫＭＳのドメイン名・公開鍵２６３を参照して、公開鍵の情報に付いている電子署名が信用するＫＭＳのものか否かを判定し、公開鍵の情報が信用できるか否かを確認する。

公開鍵問い合わせ処理部２４３は、信用するＫＭＳのドメイン名・公開鍵２６３が複数ある場合に、公開鍵を問い合わせるドメイン名に応じて信用するＫＭＳのドメイン名・公開鍵２６３の中から最適な信用するＫＭＳを選択する。ホスト２０は、初期保持データ２６内に自分のドメイン名・公開鍵２６１と上位のＫＭＳのドメイン名２６２とを持ち、公開鍵問い合わせ処理部２４３は、公開鍵を問い合わせに行く際に自分のドメイン名・公開鍵２６１と上位のＫＭＳのドメイン名２６２とを参照する。

セキュリティ通信処理部２７は、公開鍵問い合わせ処理部２４３が取得した通信相手の公開鍵に基づいて、従来の方法に従ってセキュリティ通信を行う。

次に、図４に示すフロー、及び、ホスト・ＫＭＳ間及びＫＭＳ・ＫＭＳ間でやり取りするパケットの種類とそれらに付与される電子署名を示す図８を参照して、本発明を階層的なドメイン名の構造を持つネットワークに適用した場合の図７に示すネットワークにおいて、ホストが通信相手の公開鍵の取得ために行う手順について説明する。

図７において、ＫＭＳ０(７３)、ＫＭＳ１(７２)、ＫＭＳ２(７６)、ＫＭＳ００(７４)は、図１により説明した構成を持つＫＭＳであり、また、ホストＡ７１、Ｂ７５は、図２により説明した構成の拡張したＤＮＳクライアントの機能を持つホストである。そして、ＫＭＳ００(７４)は、ドメイン名ｘｘを持つネットワーク７０１に接続され、ＫＭＳ０(７３)は、ドメイン名ａ．ｘｘを持つネットワーク７０２に接続されている。また、ホストＡ７１とＫＭＳ１(７２)とは、ドメイン名ｂ．ａ．ｘｘを持つネットワーク７０３に接続され、ホストＢ７５とＫＭＳ２(７６)とは、ドメイン名ｃ．ａ．ｘｘを持つネットワーク７０４に接続されている。

ドメイン名は、階層構造を成しており、各ＫＭＳは、従来のＤＮＳサーバの役割をも果たしている。また、図８に示す例は、ホストＢ７５の公開鍵の情報をＫＭＳ２(７６)のみが持っている場合の各ＫＭＳの動作を示しており、また、図８に示す各矢印は、ホストＡ７１がホストＢ７５の公開鍵を取得する際に、ホストとＫＭＳとの間やＫＭＳとＫＭＳとの間でやり取りするパケットやパケットに付加する電子署名の形態を示している。パケットの種類は、公開鍵問い合わせ、電子署名要求、公開鍵応答の３通りあり、電子署名の具体的な内容は、図８の枠内の記号を用いて表しているように、次のように定義されているものとする。

Ｓ（Ｋ，［ａ，ｂ，ｃ］）：鍵Ｋによりメッセージ［ａ，ｂ，ｃ］に電子署名を付与したもの

Ｄ（Ｘ）：Ｘのドメイン名

S（X）：Xの公開鍵

T（X）：Xの秘密鍵

ＩＰ（X）：XのＩＰアドレス

KMS（X）：Xが電子署名を要求するＫＭＳ

以下、ホストＡ７１が電子署名を要求するＫＭＳがＫＭＳ００(７４)であるとして図４に示すフローを説明する。

（1）まず、ホストAは、ホストＢ７５の公開鍵を問い合わせるパケットをＫＭＳ１(７２)に送信する。この公開鍵を問い合わせるパケットは、図８に矢印８１により示しているように、

S（T（A），［D（B），KMS（A），ＩＰ（A），D（A）］）

であり、これは、前述の定義から理解できるように、ホストBのドメイン名、ホストAが電子署名を要求するＫＭＳ、ホストAのＩＰアドレス、ホストAのドメイン名よりなるメッセージに、ホストAの秘密鍵により電子署名を行ったものである。ＫＭＳ１(７２)がホストＡ７１からホストＢ７５の公開鍵を問い合わせるパケットを受けたとき、図１に示す電子署名処理部１４４は、パケットに付いている電子署名を見る。電子署名処理部１４４は、ドメイン名・公開鍵・電子署名テーブル１６からホストＡ７１の公開鍵を取り出し、パケットの内容が改竄されてないか否かをその公開鍵を使って判定する（ステップ４１）。

（2）ＫＭＳ１(７２)は、ステップ４１の判定で、問い合わせパケットが改竄されていた場合、そのパケットを廃棄して処理を終了し、問い合わせパケットが改竄されていない場合、図１に示す公開鍵問い合わせ／応答処理部１４３を動作させ、問い合わせのドメイン名についてドメイン名・公開鍵・電子署名テーブル１６にエントリがあるか否か検索する。ここで、タイムスタンプも参照し、一定時間以上過ぎている場合、無効なエントリと見做す（ステップ４３、４２）。

（3）ステップ４２の判定で、ドメイン名・公開鍵・電子署名テーブル１６にエントリがなかったとき、図７に示すＫＭＳ１(７２)の公開鍵問い合わせ／応答処理部１４

３は、問い合わせのあったホストのドメイン名と自分のドメイン名とについてそれぞれが属するネットワークの名前が一致するか否か判定する。例えば、図７において、問い合わせのホストがＢ７５である場合、Ｂ７５の属するネットワークのドメイン名ｃ．ａ．ｘｘとＫＭＳ１（７２）の属するネットワークのドメイン名ｂ．ａ．ｘｘは一致しない（ステップ４４）。

（４）ステップ４４の判定においてネットワークの名前が一致したとき、図７のＫＭＳ１（７２）は、ホストＡ７１に対してホストＢに対する公開鍵が未解決であることを通知する（ステップ４５）。

（５）ステップ４４の判定においてネットワークの名前が一致しなかったとき、ＫＭＳ１（７２）は、図１にける初期保持データ１７内の上位のＫＭＳのドメイン名１７２を参照して問い合わせ先を調べ、ＫＭＳ０（７３）にホストＢ７５の公開鍵を問い合わせる。この場合の問い合わせパケットは、図８に矢印８２により示すように、

Ｓ（Ｔ（ＫＭＳ１），［Ｄ（Ｂ），ＫＭＳ（Ａ），ＩＰ（ＫＭＳ１），Ｄ（ＫＭＳ１）］）であり、ホストＢ７５のドメイン名、ホストＡ７１が電子署名を要求するＫＭＳのドメイン名、ＫＭＳ１（７２）のＩＰアドレス及びＫＭＳ１（７２）のドメイン名をメッセージとし、ＫＭＳ１（７２）の秘密鍵を電子署名の鍵とする電子署名を付加して構成される。このように、電子署名を付加することによって問い合わせパケットの不正な改竄を防止することができる（ステップ４６）。

（６）次に、ＫＭＳ１（７２）は、自ＫＭＳに公開鍵を問い合わせた者がホストかＫＭＳかを公開鍵問い合わせパケットの始点ＩＰアドレスから判定し、公開鍵を問い合わせたのがＫＭＳである場合、処理を終了する（ステップ４６１）。

（７）ステップ４６１で、自ＫＭＳに公開鍵を問い合わせた者がホストである場合、公開鍵問い合わせ／応答処理部１４３は、上位のＫＭＳから公開鍵の応答があるまで一定時間待ち、一定時間内に公開鍵の応答がなく、電子署名付きの公開鍵を取得できなかった場合、処理を終了する（ステップ４６２、４６３）。

（８）公開鍵問い合わせ／応答処理部１４３は、電子署名付きの公開鍵の応答が一定

時間内にあった場合、その公開鍵を図１に示すドメイン名・公開鍵・電子署名テーブル１６にキャッシングする。このようにキャッシングを行うことにより、別のホストから同じドメイン名について公開鍵の問い合わせがあったときに、公開鍵問い合わせ／応答処理部１４３は、再度別のＫＭＳに公開鍵の問い合わせに行かずに済み、公開鍵を解決する処理を効率的に行うことができる（ステップ４６４）。

（9）次に、公開鍵問い合わせ／応答処理部１４３は、図８の矢印８７に示すように自らの電子署名をつけた公開鍵応答パケットを公開鍵の問い合わせを受けたホストに返す。この電子署名付きの公開鍵応答パケットは、Ｄ(ＫＭＳ１)、Ｄ(Ｂ)、Ｓ(Ｂ)、Ｓ(Ｔ(ＫＭＳ００))，［Ｄ(Ｂ)，Ｓ(Ｂ)，Ｄ(ＫＭＳ００)］をメッセージとし、秘密鍵Ｔ(ＫＭＳ１)を署名の鍵とするものである（ステップ４６５）。

(10) ステップ４２のデータベースの検索で、問い合わせのドメイン名について、ドメイン名・公開鍵・電子署名テーブル１６にエントリがあった場合、図１に示す公開鍵問い合わせ／応答処理部１４３は、そのエントリに指定されたＫＭＳの電子署名が付いているか否かを見る（ステップ４７）。

(11) ステップ４７のチェックで、指定されたＫＭＳの電子署名がエントリに付いていた場合、公開鍵問い合わせ／応答処理部１４３は、そのエントリにある電子署名付きの公開鍵をホストＡ７１に返す（ステップ４８）。

(12) 一方、ステップ４７で指定されたＫＭＳの電子署名がエントリに付いていなかった場合、公開鍵問い合わせ／応答処理部１４３は、パケットに付いているホストＡ７１が信用するＫＭＳと図１の初期保持データの上位のＫＭＳのドメイン名１７２を見て、図７に示すＫＭＳ０(７３)に電子署名の要求を出す。図７に示すＫＭＳ２(７６)がホストＢ７５の公開鍵の情報を持っていて、ＫＭＳ０(７３)に電子署名の要求を出す場合、図８の矢印８４に示すように、［Ｄ（Ｂ）、ＫＭＳ（Ａ）、ＩＰ（ＫＭＳ１）、Ｓ（Ｂ）及びＤ（ＫＭＳ２）］をメッセージとして、ＫＭＳ２(７６)の秘密鍵を鍵とする電子署名を付けて要求を行う（ステップ４９）。

前述では、図７におけるＫＭＳ１(７２)の動作について説明したが、他のＫＭＳ

０（７３）、ＫＭＳ２（７６）も、前述したＫＭＳ１（７２）の場合と同様な動作を行う。

次に、図５に示すフローと図７及び図８とを参照して、図１に示すＫＭＳの各部の動作の中での電子署名の要求と応答とについて説明する。

（１）いま、図７に示すＫＭＳ０（７３）が、ＫＭＳ１（７２）から電子署名の要求を受けたとする。この場合、ＫＭＳ０（７３）は、図１に示すような構成を持つ自装置内の電子署名処理部１４４を動作させ、パケットに付いている電子署名を見る。電子署名処理部１４４は、ドメイン名・公開鍵・電子署名テーブル１６からＫＭＳ１７２の公開鍵を取り出し、パケットの内容が改竄されていないか否かを判定する（ステップ５１）。

２）ステップ５１の判定で、パケットの内容が改竄されていた場合、電子署名処理部１４４はパケットを廃棄し、ＫＭＳ０（７３）は処理を終了する（ステップ５３）。

（３）ステップ５１の判定で、パケットの内容が改竄されていなかった場合、電子署名処理部１４４は、パケットの内容を見て電子署名の要求先が自分自身か否かを判定する（ステップ５２）。

（４）ステップ５２の判定で、電子署名の要求先が自分自身でない場合、電子署名処理部１４４は、初期保持データの上位のＫＭＳのドメイン名１７２を参照し、電子署名の要求を上位のＫＭＳに対して出す。図７において、ホストＡ７１が電子署名を要求するＫＭＳがＫＭＳ００（７４）である場合、図８の矢印８５に示すように、ＫＭＳ０（７３）からＫＭＳ００（７４）への電子署名要求パケットは、［Ｄ（Ｂ）、ＫＭＳ（Ａ）、ＩＰ（ＫＭＳ１）、Ｓ（Ｂ）及びＤ（ＫＭＳ０）］をメッセージとしＫＭＳ０（７３）の秘密鍵を鍵とする電子署名を付けたものとなる（ステップ５４）。

（５）一方、ステップ５２の判定で、電子署名の要求先が自分自身であった場合、電子署名処理部１４４は、要求されたパケットに対して自分の秘密鍵によって電子署名を付け、要求元のＫＭＳに電子署名付きのパケットを返す。説明している例で、例えば、署名要求に対してＫＭＳ００（７４）がＫＭＳ１（７２）へ公開鍵を応答するものとすると、その場合の応答パケットは、図８の矢印８６に示すように、［Ｄ（Ｂ）、Ｓ（Ｂ）及びＤ（ＫＭＳ００）］をメッセージとしＫＭＳ００（７４）の秘密鍵を鍵とす

る電子署名を付けたものとなる（ステップ５５）。

次に、図６に示すフローと図７及び図８とを参照して、図２に示す構成のホストの動作を説明する。

（１）図７において、ホストＡ７１がホストＢ７５の公開鍵を取得しようとするものとする。このとき、図２に示す構成を持つホストＡ７１の公開鍵問い合わせ処理部２４３は、ドメイン名・公開鍵・電子署名テーブル２５を検索しホストＢ７５のエントリがあるか否かを調べる（ステップ６１）。

（２）ステップ６１で、ドメイン名・公開鍵・電子署名テーブル２５にホストＢ７５のエントリがなかったとき、公開鍵問い合わせ処理部２４３は、初期保持データ２６の信用するＫＭＳのドメイン名・公開鍵２６３を参照して信用するＫＭＳを選択し、信用するＫＭＳのドメイン名・公開鍵２６３が複数ある場合、問い合わせるドメイン名より上位にあってそれに最も近いＫＭＳを選択する（ステップ６２）。

（３）次に、公開鍵問い合わせ処理部２４３は、初期保持データ２６内の公開鍵を問い合わせに行くＫＭＳのドメイン名２６２を参照して、そのＫＭＳにホストＢ７５の公開鍵を問い合わせる。この場合の公開鍵問い合わせパケットは、図８の矢印８１に示すように、［Ｄ（Ｂ）、ＫＭＳ（Ａ）、ＩＰ（Ａ）及びＤ（Ａ）］をメッセージとし、ホストＡの秘密鍵Ｔ（Ａ）を鍵とする電子署名を付加したものとなる（ステップ６３）。

（４）ホストＡ７１は、ステップ６３での問合せに対して、公開鍵応答パケットが返ってきたとき、図２の電子署名確認部２４４を動作させ、公開鍵応答パケットに付いている電子署名が要求したＫＭＳのものであって、かつパケットの内容が改竄されていないかを確認する（ステップ６４）。

（５）一定時間以内に公開鍵応答パケットが返ってこないとき、あるいは、ステップ６４で、公開鍵応答パケットに付いている電子署名が要求したＫＭＳのものでないか、パケットの内容が改竄されていると判定された場合、ホストＡ７１は、何もせずに処理を終了する。これにより、ネットワーク上にある不正なホストが自らの公開鍵とア

ドレスが問い合わせのあったドメイン名に対応しているように見せかけることでセキュリティ通信の相手になりすますことを防止することができる。

（６）ステップ６４で、公開鍵応答パケットに付いている電子署名が要求したＫＭＳのものであって、かつパケットの内容が改竄されていないと判定された場合、公開鍵問い合わせ処理部２４３は、その公開鍵応答パケットの内容を見て、ドメイン名・公開鍵・電子署名・署名したＫＭＳのドメイン名の４つの組でドメイン名・公開鍵・電子署名テーブル２５にキャッシングする（ステップ６５）。

（７）ホストＡ７１のセキュリティ通信処理部２７は、前述までの処理で取得した公開鍵、あるいは、ステップ６１で見つかった公開鍵を用い、セキュリティ通信を行うための処理を開始する（ステップ６６）。

ホストは、前述した処理を実行することにより、公開鍵を解決する処理を効率化することができる。

前述した本発明の実施形態によれば、ネットワークの２つのホストがセキュリティ通信を開始する前に機能拡張したＤＮＳサーバによって通信相手のホストのドメイン名に対応する公開鍵を自動的に取得させることが可能となり、公開鍵の管理の容易化を図ることができる。

また、本発明の実施形態によれば、ホストが指定したＤＮＳサーバによって公開鍵の応答パケットに電子署名を付けさせることができるので、ネットワーク上にある不正なホストが自らの公開鍵とアドレスとが問い合わせのあったドメイン名に対応しているように見せかけることによりセキュリティ通信の相手になりすますことを防止することができる。

前述したような本発明は、ＦＤやＣＤ－ＲＯＭ等の記憶媒体に本発明を実現するプログラムを格納しておき、このプログラムをＤＮＳサーバ及びホストにインストールして実現することができる。また、本発明は、ネットワークに接続された情報処理装置の記憶媒体に本発明を実現するプログラムを格納しておき、ネットワークを通してＤＮＳサーバ及びホストのハードディスク等の記憶媒体に前述のプログラムをコ

ピーして実現することができる。

CLAIMS

1．　階層構造を持ち、各階層毎にドメイン名を持つネットワークと、そのドメイン名とアドレスとの対応を管理する前記各階層毎に設けられるＤＮＳサーバと、ネットワークに収容されるホストとを備え、前記ＤＮＳサーバが、ネットワークに属するホストに対して他のホストが持つ公開鍵を配布する公開鍵管理方法において、前記ＤＮＳサーバは、公開鍵を管理する手段と、前記ネットワークに属するホストの公開鍵とドメイン名とを対応付けて格納したデータベースとを持ち、第１のホストからのドメイン名の情報による第２のホストの公開鍵の問い合わせを受けたとき、前記公開鍵管理手段が前記データベースを参照することにより、前記ドメイン名に対応する第２のホストの公開鍵の情報を前記第１のホストに応答することを特徴とする公開鍵管理方法。

2．　前記ＤＮＳサーバは、第１のホストから第２のホストの公開鍵の問い合わせを受けたとき、自サーバ内の前記データベースの中に問い合わせのドメイン名に対応するエントリがない場合、他の公開鍵管理手段とデータベースとを備えた他のＤＮＳサーバに公開鍵の解決をドメイン名の階層に沿って再帰的に委託することを特徴とするクレーム１の公開鍵管理方法。

3．　前記ホストは、前記ＤＮＳサーバに他のホストの公開鍵を問い合わせる手段を備え、セキュリティ通信開始時、前記公開鍵問い合わせ手段に通信相手となるホストのドメイン名に対応する公開鍵を前記ＤＮＳサーバに問い合わせることを特徴とするクレーム１の公開鍵管理方法。

4．　クレーム１の公開鍵管理方法を実現するための、ＤＮＳサーバに設けられる公開鍵を管理する手段の機能を実行するプログラムと、ネットワークに属するホスト

の公開鍵とドメイン名とを対応付けて格納するデータベースと、ホストからドメイン名の情報によって公開鍵の問い合わせを受けたとき該公開鍵管理手段が前記データベースを参照することによりドメイン名に対応する公開鍵をホストに応答する処理を実行するプログラムとを格納したことを特徴とする記憶媒体。

ABSTRACT OF THE DISCLOSURE

階層構造のドメイン名の構成を持ち、そのドメイン名とアドレスとの対応を管理するＤＮＳサーバが階層毎にあるネットワークにおいて、公開鍵を管理するモジュールとネットワークに属するホストの公開鍵とドメイン名との対応を示すデータベースを各ＤＮＳサーバに設ける。２つのホストがセキュリティ通信を開始するとき、一方のホストが前述の機能拡張したＤＮＳから通信相手のホストの公開鍵を自動的に取得する。このとき、公開鍵問い合わせパケットの中にホストが信用するＤＮＳサーバの名前を入れさせ、このホストが指定するＤＮＳサーバが、公開鍵応答パケットに電子署名を付ける。ホストは、この電子署名により公開鍵応答パケットにある公開鍵が信用できるかどうかを判定することができ、不正なホストが通信相手になりすますのを防止する。

E5272-01

図1

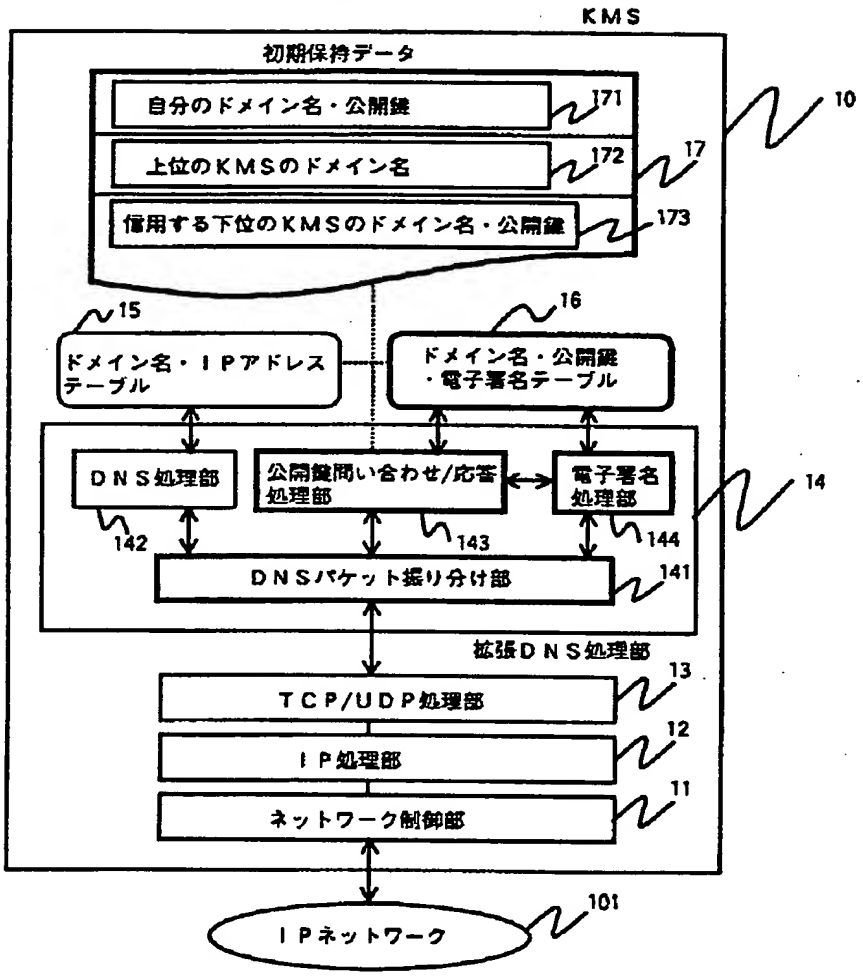


図２

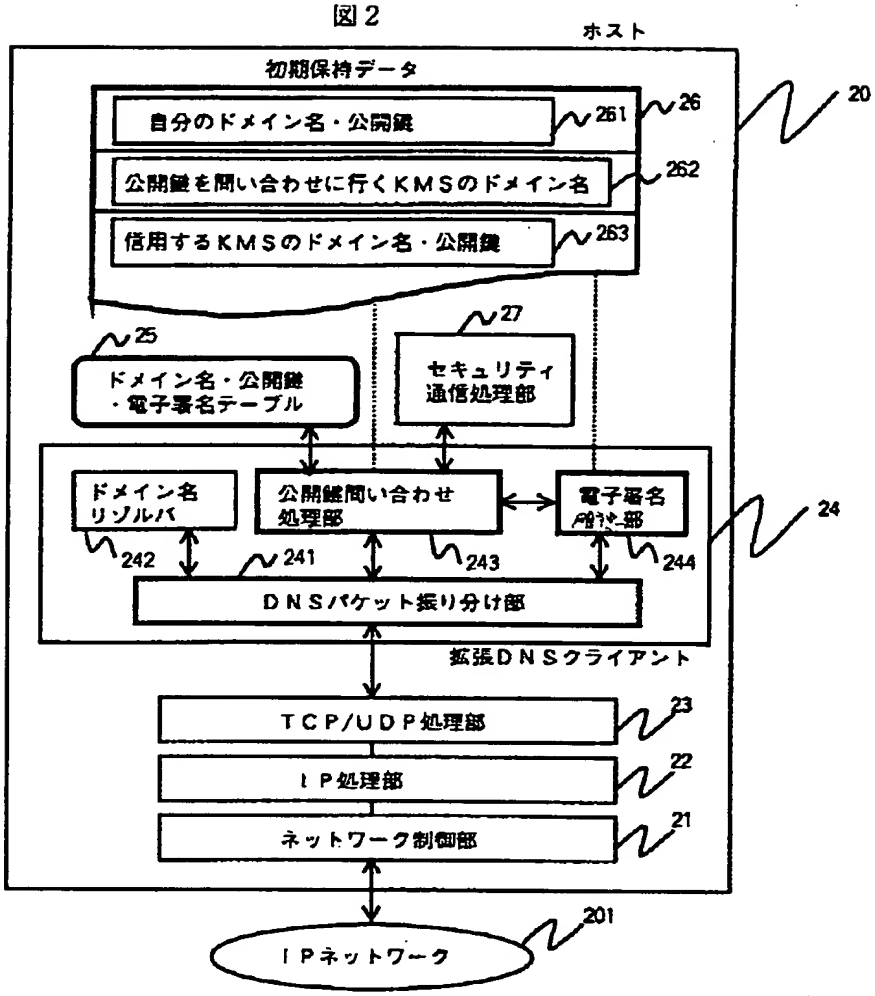


図３

31 ドメイン名	32 公開鍵	33 電子署名	34 電子署名を付けたKMS名	35 タイムスタンプ

図4

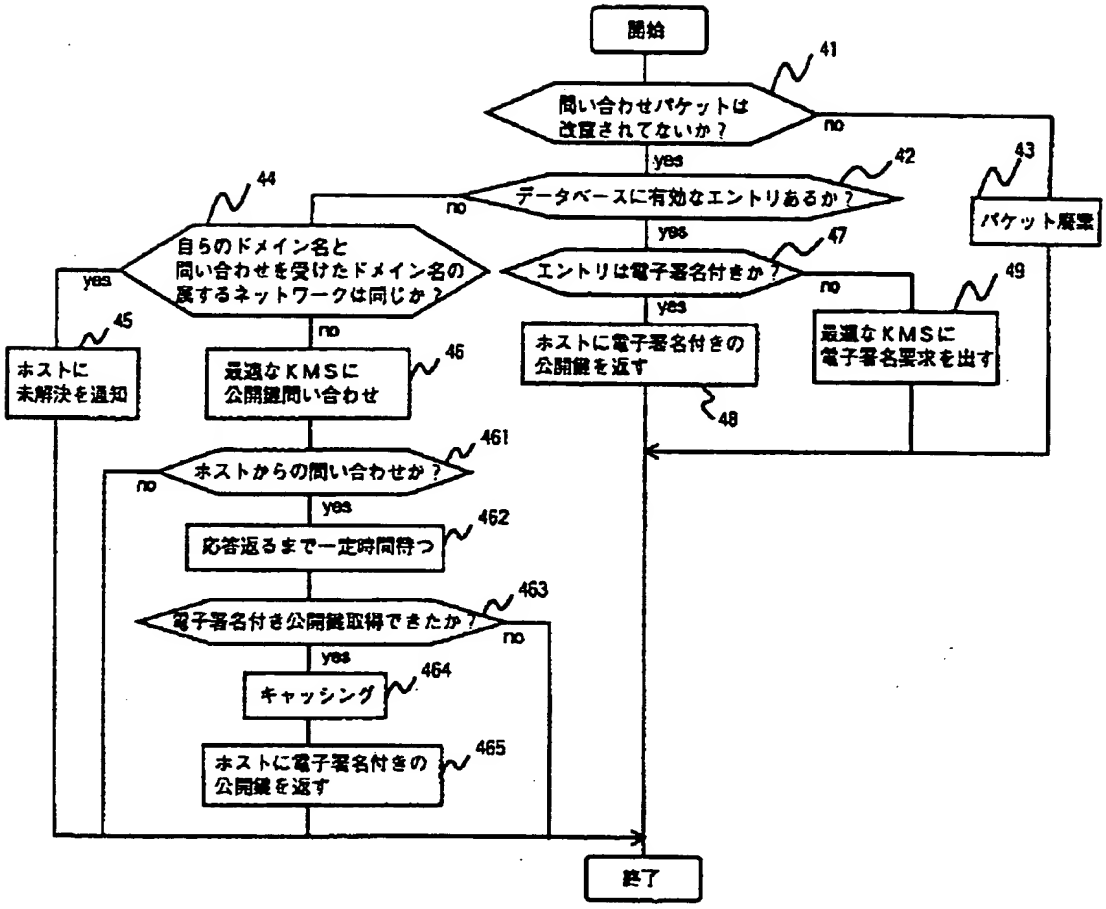

開始
41
問い合わせパケットは改竄されてないか？
no
yes
42
データベースに有効なエントリあるか？
43
パケット廃棄
no
yes
44
自らのドメイン名と問い合わせを受けたドメイン名の属するネットワークは同じか？
47
エントリは電子署名付きか？
yes
no
49
最適なKMSに電子署名要求を出す
45
ホストに未解決を通知
no
46
最適なKMSに公開鍵問い合わせ
ホストに電子署名付きの公開鍵を返す
48
461
ホストからの問い合わせか？
no
yes
462
応答返るまで一定時間待つ
463
電子署名付き公開鍵取得できたか？
no
yes
464
キャッシング
465
ホストに電子署名付きの公開鍵を返す
終了

図5

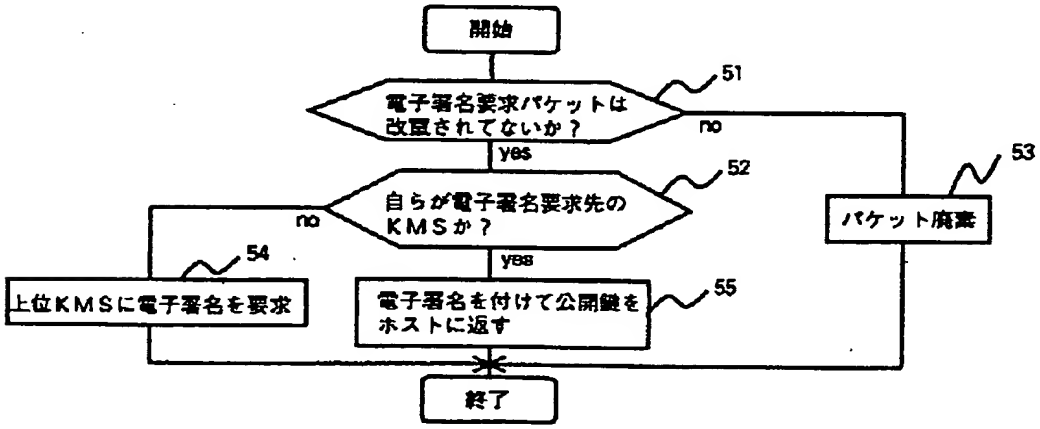

開始
51
電子署名要求パケットは改竄されてないか？
no
yes
52
自らが電子署名要求先のKMSか？
53
パケット廃棄
no
yes
54
上位KMSに電子署名を要求
電子署名を付けて公開鍵をホストに返す
55
終了

図6

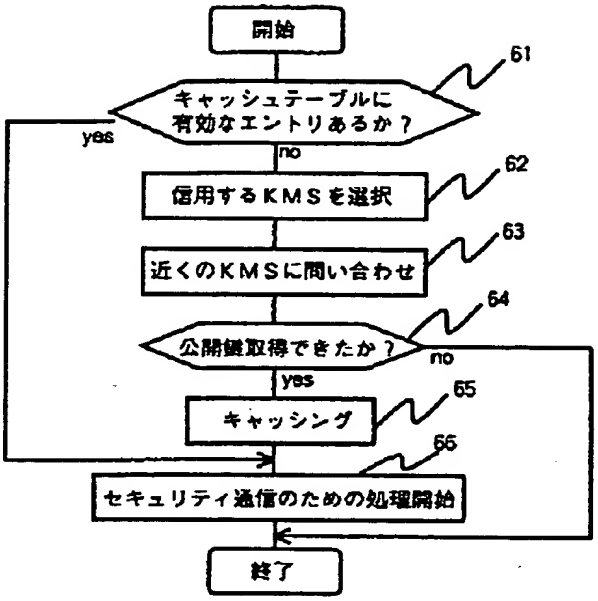

開始
キャッシュテーブルに
有効なエントリあるか？
61
yes
no
信用するKMSを選択
62
近くのKMSに問い合わせ
63
公開鍵取得できたか？
64
no
yes
キャッシング
65
セキュリティ通信のための処理開始
66
終了

図7

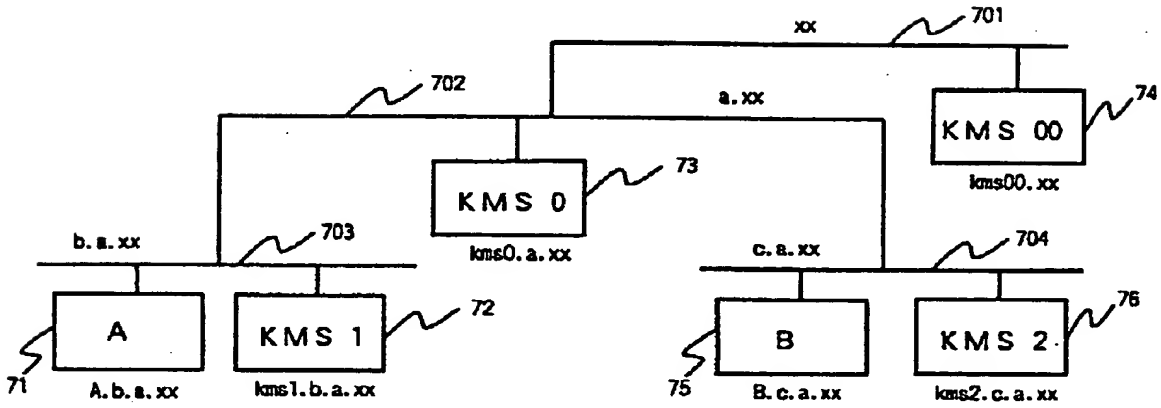
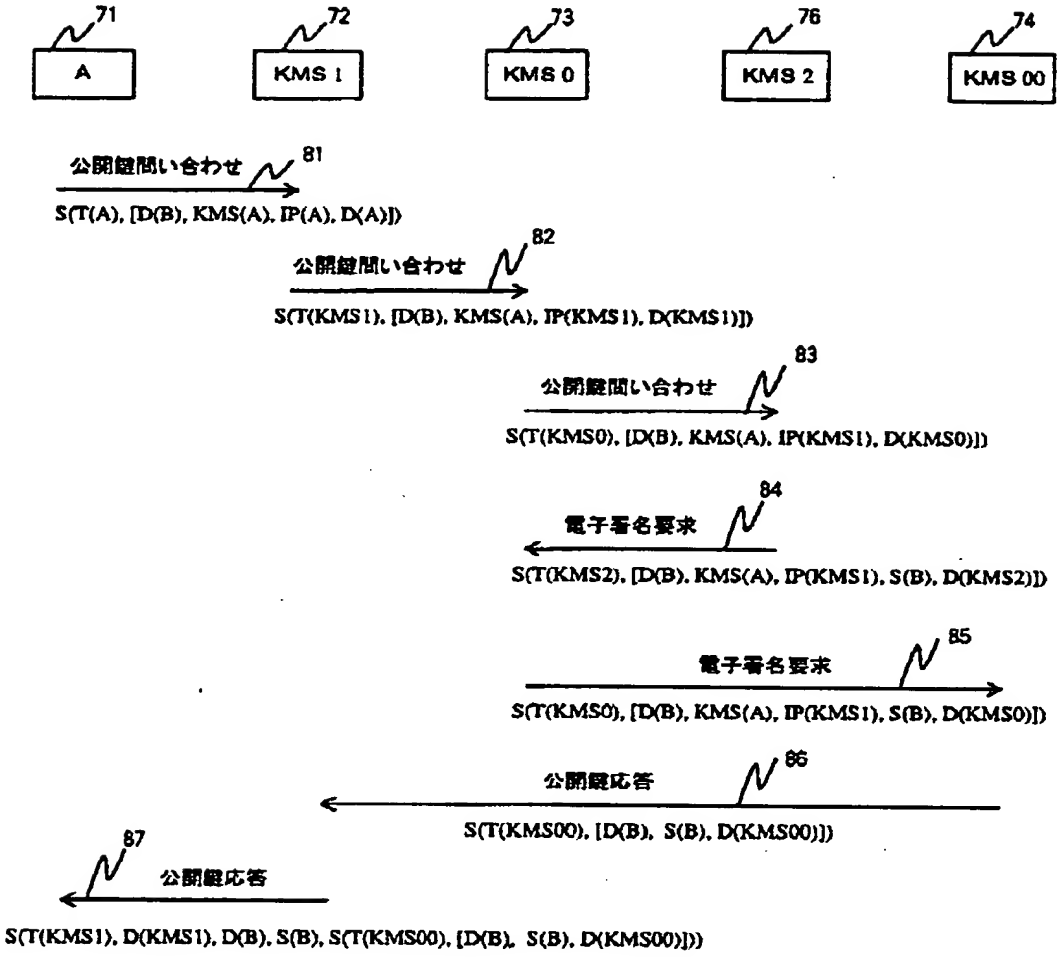

xx
701
a.xx
702
KMS 00
74
kms00.xx
KMS 0
73
kms0.a.xx
b.a.xx
703
c.a.xx
704
A
71
A.b.a.xx
KMS 1
72
kms1.b.a.xx
B
75
B.c.a.xx
KMS 2
76
kms2.c.a.xx

図 8



D(X) : Xのドメイン名
S(X) : Xの公開鍵
T(X) : Xの秘密鍵
IP(X) : XのIPアドレス
KMS(X) : Xが電子署名を要求するKMS

S(K, [a, b, c]) : 鍵Kでメッセージ [a, b, c] に電子署名をつけたもの

図９

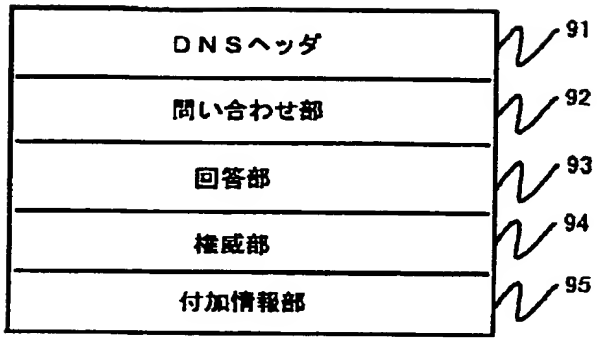
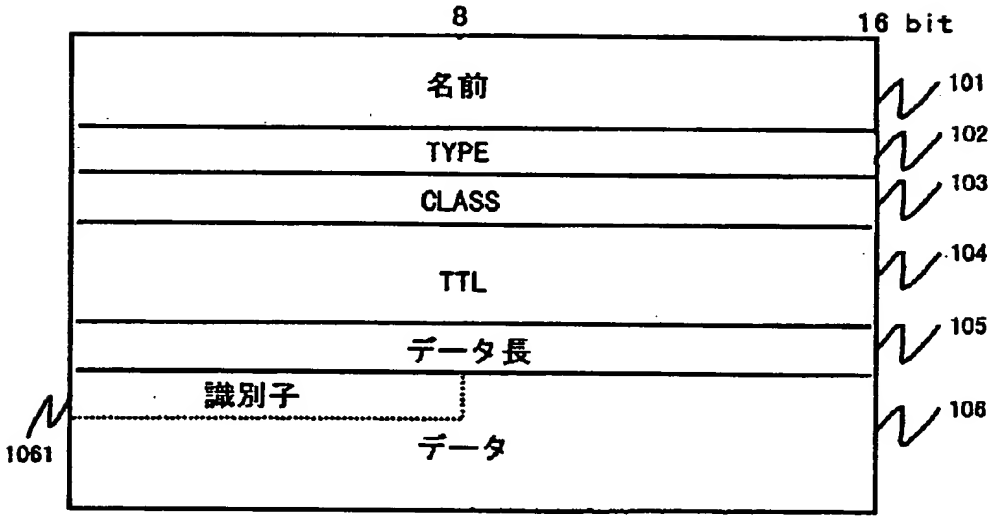

ＤＮＳヘッダ
問い合わせ部
回答部
権威部
付加情報部
91
92
93
94
95

図１０


8
16 bit
名前
TYPE
CLASS
TTL
データ長
識別子
データ
1061
101
102
103
104
105
106